Elements of the Government of Mexico for the United Nations *ad hoc* Committee to elaborate a comprehensive international Convention on countering the use of information and communications technologies for criminal purposes

For the Government of Mexico, information and telecommunications, digital technologies and the cyberspace offer great opportunities to enhance development, close inequality gaps, to promote inclusion, well-being, justice and overall human rights.

Mexico recognizes, at the same time, that increasing threats, crimes and the spread of an illicit market through these technologies represents a serious concern for governments, private sector, civil society and all citizens.

International cooperation, mechanisms for legal assistance and information exchange are more necessary than ever. Mexico is committed to multilateralism, and especially to the role of the United Nations, to generate comprehensive and meaningful responses to this global challenge.

The Government of Mexico considers that the mandate by the General Assembly for the elaboration of a comprehensive Convention against the use of information technologies for criminal purposes constitutes an ideal opportunity to achieve a substantive, committed, plural, inclusive and transparent process. It is expected that such negotiation process builds upon the lessons learned from other related United Nations processes, and from other related regional experiences.

Taking into account the positive expectations of the Government of Mexico on this multilateral process, and after consolidating a national inter-agency consultation, the following elements are presented to consider to frame of preparations and the contents of the future Convention:

Elements on the general approach and scope of Convention
The Convention must be a comprehensive binding legal instrument, which includes substantive and procedural aspects, aimed at establishing basis for international cooperation and the exchange of information, experiences, capacities and best practices. It is expected to contribute to promote standards to improve investigation, mitigation and prosecution considering national laws and practices. It is expected that although the Convention does not exclude the possibility of signing other international instruments on the matter, it will be a benchmark for having an approved scheme that makes the prosecution of cybercrimes more efficient. It is considered that it should incorporate: • General definitions, very basic typologies and competent actors. • Basic procedural measures that States must have for the adequate investigation and prosecution of cybercrimes. • General suggested offenses that should be considered by respective national laws. • Mechanisms for accessing information and promoting operational collaboration. It would be desirable that the future Convention allows the formulation of reservations and interpretative declarations, also that it contains a flexible amendment procedure to facilitate its updating and that it establishes mechanisms to settle disputes. It will be convenient that the entry into force is subject to the deposit of 50 instruments of ratification. Once having certainty of the content of the Convention, it will be useful to agree on an efficient, universal, peer-to-peer, inclusive and non-onerous mechanism for review of implementation.

Elements on the relevance of other international instruments

For the government of Mexico, it is important that the Convention reaffirms the applicability of International Law to cyberspace and to use of information and telecommunications technologies. For this reason, it will be important for the discussions to take into considerations existing developments from various international legal instruments, such as:

• United Nations Convention against Transnational Organized Crime and its three complementary Protocols.
• Statute of the International Court of Justice.
• Convention on Cybercrime of Council of Europe.
• International treaties on human rights, and those that safeguard the guarantees of the people who intervene in jurisdictional processes.
• Treaties on protection and cross-border flow of personal data.
• Treaties applicable to intellectual property.
• Bilateral treaties on extradition, mutual legal assistance in criminal matters and other forms of international legal cooperation.

Mexico also values that documents adopted within the UN and other relevant international forums can contribute to guide discussions and negotiations, mainly:

• Compilation of conclusions and recommendations arising from the meetings of the Intergovernmental Group of Experts in charge of carrying out a comprehensive study on cybercrime, in 2018, 2019 and 2020.
• Final Report of the Group of Government Experts (GGE) to advance responsible behavior of States in cyberspace, 2019-2021, and previous.
• Final Report of the Open Ended Working Group (OEWG) on advancements in the field of information and telecommunications in the context of international security, 2019-2021.
• Resolutions of the UN General Assembly on the right to privacy in the digital age.
• Resolutions of the Human Rights Council on the promotion, protection and enjoyment of human rights online.
• Draft guidelines for the use of the Global Cybersecurity Agenda (ACG) by the International Telecommunications Union (ITU).

Elements on cybercrimes, offenses and criminal behaviours that should be addressed

For the government of Mexico, the Convention should emphasize those behaviours recognized by international law as illegal (in the terms provided in other treaties adopted within the framework of the United Nations), which are carried out by electronic and digital means.

It is not expected that the Convention will include an exhaustive catalogue of crimes, nor that all the typologies to be homologated to the different legal systems. Nevertheless, it is recommended that in the process of elaboration a dialogue can be generated as a general reference for the following cases:

• Theft and identity theft.
• Fraud and extortion.
• Ransomware.
• Malware and criminal behaviour related to the production, storage, distribution, commercialization and execution of malicious code.
• Exposure of personal or institutional information to the detriment of its owners.
• Crimes related to human trafficking, child pornography and violations of sexual privacy.
• Digital violence, including gender and hate, racial, nationality, religion or political based hostility.
• Grooming and cyberbullying.
• Attacks through vectors (phising, vishing, smishing, pharming).
• Crimes against national sovereignty, such as terrorism, sabotage, espionage and intrusion into systems with confidential information for reasons of national security.

• Criminal acts against critical information infrastructures and against the confidentiality, integrity and availability of information.
• Crimes against children.
• Violation of freedom of speech.
• Crimes committed against intellectual property.
• Crimes against banking and financial systems.
• Illicit sale of weapons, animals, controlled drugs and those that do not have a sanitary registration.
• Forgery of currency and official documents.
• Use of cryptocurrencies and dual-use assets for criminal purposes.
• Illegal modification of portals (defacement).
• Liability of legal persons.

While drafting the convention, It would be convenient to share experiences on whether sanctions will be admitted for carrying out of attempted crimes, as well as determinants that aggravate the criminal act and increase the penalties.

Elements related to sovereignty and national jurisdiction

For Government of Mexico it is important to consider to de discussions:
• To reaffirm respect for national sovereignty and the principle of non-intervention in the internal affairs of each State.
• To establish general rules for determining the applicable jurisdiction, taking as a reference similar provisions of other legal instruments and processes.
• To generate common measures to obtain traffic and content data, and to prevent the illegal interception or blocking of data.
• To advance mechanisms that give certainty to the obtaining and conservation or preservation of digital evidence, as well as its delivery.
• To clarify investigation procedures such as subpoenas or apprehensions.
• To develop specifications for the delivery of technical data and content in criminal investigations, and for the expedite dissemination of computer data.
• To address possible legal obligations of technology operators, service providers and Internet content to deliver information to the competent authorities during an investigation, regardless of their physical location.

Elements on information exchange and international cooperation

For the Mexican government, one of the main purposes of the Convention should be to generate certainty for the exchange of information and international cooperation, and to establish processes for its effective execution. It is expected that the Convention will address, among other aspects:

• Mutual legal assistance.
• Extradition.
• Common mechanisms for the request, response, reception and exchange of information for investigation and intelligence purposes.
• Judicial control procedures that allow agile and effective collaboration during the investigation.
• Cooperation to carry out police investigation procedures and obtain testimonies for judicial processes, also considering the use of information and communication technologies.
• Preparation of guides, standards, methodologies and best practices for the prevention and investigation of cybercrimes.
• Fostering collaboration between National CERTs or CSIRTs for the prevention of cybercrimes.
• Possibilities for coordinated investigations.
• Recommend a minimum common framework for the protection of information and transparency, so that despite the different policies that each State has at the national level, data from investigations and judicial processes can be shared.
• Establishing minimum periods for data conservation and digital evidence preservation.

• Consider general rules and terms to which the intervention actions of private communications and geolocation in real time must be subject.
• Establishing general parameters on regulation of privacy policies.
• Promote the standardization of local, regional and global statistics on cybercrimes.

Elements on the protection and exercise of Human Rights

All the measures to be implemented from the future Convention must be consistent with the obligations contained in international human rights instruments. It is further expected that its provisions will be compatible with the rules related to freedom of speech.

The government of Mexico hopes that in the process of drafting the Convention the following will be addressed:

• Concepts and developments related to businesses and human rights.
• Privilege the investigation, prosecution and penalization of gender violence, and crimes against girls, boys and adolescents through the Internet.
• Promote the investigation, prosecution and penalization of racist and extremists behaviours that incite violence, exclusion or segregation of people.
• Minimum common elements about net neutrality.
• Recommend mechanisms for the protection of information by Internet service companies.

Elements related to capacity building and technical assistance

The government of Mexico considers that for the effective implementation of the future Convention, it will be necessary to establish provisions that promote capacity building, both for the prevention and prosecution of cybercrimes. In this regard, the following elements are expected to discuss and agree on:

• Advance training efforts, technical assistance and sharing best practices, as well as standardized procedures to perform computer forensics and obtain valid digital evidence.
• Promote education initiatives for prevention and replicable public awareness campaigns.
• Also promote the creation or strengthening of CERTs in various sectors, such as financial, academic, commercial and energy.
• Prepare guides, guidelines and recommendations that promote the adoption of best practices.
• Expand the catalogue of trainings focused on different interested groups: investigators, researchers, prosecutors, judges, diplomats, legislators, and non-state actors.

Elements on the participation of relevant non-state actors (civil society, private sector, academia)

For the government of Mexico, it is convenient that, from the very process of preparing the Convention, mechanisms are sought to facilitate the participation and submission of inputs from civil society organizations, the private sector, service providers, academia and research centers. It will be desirable to consider:

• The possible involvement of these actors in the processes to prevent and fight cybercrime.
• Promote collaborative environments with private CERTs, Carriers and various telecommunications companies.
• Dialogue with the private sector that operates critical information infrastructures or that are within strategic sectors, as well as with companies that provide free Internet services such as email, instant messaging, micro-blogs and online transportation services.
• Support self-regulation and social awareness measures, as well as promote the inclusion of the concepts of business and human rights.